

AMENDMENTS TO THE CLAIMS:

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Cancelled).
2. (Currently amended) The mobile Mobile telephone handset according to claim [[1]] 18, wherein the operating system controls the transmission of the IMEI to a mobile telephone operator by means of a secure OTA channel.
3. (Cancelled).
4. (Currently amended) The handset Handset according to claim [[1]] 18, wherein the secure electronic module second data storage device is a UICC.
5. (Currently amended) The handset Handset according to claim [[1]] 18, wherein the operating system controls the authentication of the secure module second data storage device by the storage support first data storage device.
6. (Currently amended) The handset Handset according to claim 5, wherein the secure electronic module second data storage device and the storage support first data storage device store encryption keys that are used adapted to securing encrypt the secure communication channel.

7. (Currently amended) The handset Handset according to claim [[1]] 18, wherein the secure module second data storage device blocks the use of the handset when a false IMEI is detected.
8. (Cancelled).
9. (Currently amended) The method of Method according to claim [[8]] 19, wherein the secure module second data storage device also transmits the IMEI to a mobile telephone operator over a secure OTA channel.
10. (Currently amended) The method of Method according to claim 9, wherein the operator compares the IMEI with a black list of stolen handsets, and blocks the communications of the handset when the handset appears on the black list.
11. (Currently amended) The method of Method according to claim [[8]] 19, wherein the secure module second data storage device blocks the use of the handset when a false IMEI is detected.
12. (Currently amended) The handset Handset according to claim 4, wherein the operating system controls the authentication of the secure module second data storage device by the storage support first data storage device.

13. (Currently amended) The handset Handset according to claim 4, wherein the ~~secure module~~ second data storage device blocks the use of the handset when a false IMEI is detected.

14. (Currently amended) The handset Handset according to claim 5, wherein the ~~secure module~~ second data storage device blocks the use of the handset when a false IMEI is detected.

15. (Currently amended) The handset Handset according to claim 6, wherein the ~~secure module~~ second data storage device blocks the use of the handset when a false IMEI is detected.

16. (Currently amended) The method of Method according to claim 9, wherein the ~~secure module~~ second data storage device blocks the use of the handset when a false IMEI is detected.

17. (Currently amended) The method of Method according to claim 10, wherein the ~~secure module~~ second data storage device blocks the use of the handset when a false IMEI is detected.

18. (New) A telephone handset, comprising:

a first data storage device storing an International Mobile Equipment Identity (IMEI) associated with an operator of a communication network;

a second data storage device;

a processor;

a memory device including program instructions that, when executed by the processor, control the handset to:

authenticate, by the second data storage device, the first data storage device;

establish, based on said authentication, an encrypted communication channel between the first data storage device and the second data storage device;

transmit, via the encrypted communication channel, the IMEI from the first data storage device to the second data storage device; and

enable the handset to access the communication network based on the IMEI received by the second data storage device.

19. (New) A method of securing a telephone handset, said method comprising:

authenticating a first data storage device by a second data storage device, said first data storage device storing an International Mobile Equipment Identity (IMEI) associated with the operator of a communication network;

establishing, by a processor based on said authentication, an encrypted communication channel between the first data storage device and the second data storage device;

transmitting, by the processor via the encrypted communication channel, the IMEI from the first data storage device to the second data storage device; and

enabling, by the processor, the handset to access the communication network based on the IMEI received by the second data storage device.

20. (New) A telephone handset, comprising:

a first encrypted data storage device storing an International Mobile Equipment Identity (IMEI) associated with the operator of a communication network;

a second encrypted data storage device;

means for authenticating the first data storage device by the second data storage device;

means for establishing, based on said authentication, an encrypted communication channel between the first data storage device and the second data storage device;

means for transmitting, via the communication channel, an IMEI from the first data storage device to the second data storage device; and

means for enabling the handset to access the communication network based on the IMEI received by the second data storage device.